Instructions of Technical and Technological Requirements for the Electronic Payment and Money Transfer Companies No. (8 /2018)

Issued Pursuant to the provisions of paragraphs (d) and (e) of article (5), provisions of paragraph (e) of article (6) and provisions of paragraph (a) of article (48) and article (55) of the bylaw of Electronic Payment and Money Transfer No. (111) for 2017

Article (1):

These Instructions are called "Instructions of Technical and Technological Requirements for the electronic Payment and money Transfer companies" and shall enter into force from the date of its approval.

Article (2):

A) Wherever they should occur herein, The following words and terms shall have the meanings assigned to each hereunder, unless otherwise connoted by the context:

Information and communications technology environment	: The group of computerized equipment related to internal and external networks, main servers and operating software on it and all supporting systems in the company's main site and disaster recovery site.
Information Assets:	Any information, electronic or none electronic files, devices or storage media, programs or any components of information and communications technology environment's related to the company activities.
Sensitive data :	Confidential and/ or top secret data which are considered of utmost importance to the company and exposes its security, privacy and the people dealing with it to serious danger.

B) The definitions stated in the effective bylaw of the electronic payment and money transfer wherever it is provided in these instructions shall be adopted unless the context provides otherwise.

Application Scope

Article (3):
The provision of these Instructions shall apply towards all of the following parties:

A) The Operating companies in the Kingdom which are licensed by the Central Bank, including branches of the foreign companies to practice any of the activities of payment services or managing and operating the electronic payment system.

B) The operating banks in the Kingdom, and the exchange companies which practice any of the payment services activities or managing and operating the electronic payment systems to the extent of not being contradictory with the regulatory legislations thereof.

Article (4):
Upon applying the provisions of these Instructions, due observance should be observed in all of what has been provided in adaptation with Instructions of Cyber Risks Resilience and shall be integrally read therewith.

Requirements of the Information and Communications Technology Environment

Article (5):
A) The company should provide the necessary information and communications technology environment for providing the payment services or managing and operating the electronic payment systems and provide the support and maintenance necessary thereto.

B) The company should configure the settings of the operating systems, databases network devices and all components of the information and communications environment technology including the security settings and document them to ensure its operability with availability, integrity and reliability.

C) The company should review the components of the information and communications technology environment periodically including the methods of protection and procedures followed in the execution of operations to ensure its validity, improve and update its performance continuously as well as documenting that.

Article (6):

The company should, prior to moving to the production environment, undertake the following:

A) Examine the components of information and communication technology environment to ascertain the extent of its sufficiency, reliability and authenticity to carry out the object required and document that.

B) Change the accompanying password for all components of the new information and communications technology environment (Default Passwords) immediately upon its first use.

C) Comprehensive documentation of all components of the information and communications technology environment, and review it continuously and provide suitable protection thereto.

Protection Requirements of the Information and Communications Technology environment

Article (7):
The company must adhere to the following:

A. Utilize safe communication channels with suitable bandwidth to accommodate the volume of the exchanged data.

B. Utilize high speed communication channels to support the real time update.

C. Employ the virtual and/or physical separation techniques in as much as possible.

D. Utilize the necessary networking protection devices for the information and communications technology environment, for example without being limited to (Firewalls, intrusion detection and prevention systems).

E. Setting controls and standards for the Remote Access in the Company's networks.

Article (8):

A) The company should update the operating systems and the software installed on the devices and servers of the information and communications technology environment by the latest updates recommended by the supplying company with the necessity of conducting the necessary

examinations prior to such updating and provide effective alternative controls in case of the impossibility of same.

B) The company should delete any software or stored files on the devices and the servers that has no relation with the systems in use by the company.

Article (9):
The company should install the antivirus protection systems on the servers and employee's devices in the company and update them continuously, and set the automatic anti-virus scheduling scanning on the servers and employees' devices periodically.

Separation of Work Environments

Article (10):

A) The company should separate the production environment from other environments with due observance of the following:

1) Specify and document the software transmission rules from the test and development environment (if any) to the production environment.

2) Test environment should mimic the production environment as much as possible.

B) The Company should not permit the programing and development staff to work on the production environment except in exceptional cases provided that, they are granted temporary usernames and passwords to be changed after the end of the object therefrom for which it was granted and to document and monitor all these steps.

Access Management

Article (11):

A) The Company should place suitable controls in order to manage the Logical Access to the information environment and communications technology pertaining thereto, and to test it continuously, provided that it include as a minimum the following:

1) Utilize strong and effective access controls depending on the risks level, and using the necessary tools and techniques so as to ensure accountability and non-repudiation.

2) Official procedures for the processes of allocating multi access rights to the new users and the process of deleting and revoking such rights for

the various systems of information and communications technology environment.

3) Allocating access rights as need-to-use only and for every utilization separately, provided it is reviewed periodically with due observance to the privileged access rights that with higher confidentiality and privacy.

4) Restrict the number of the utilized user IDs to access, and utilize the company's various systems from those of high privileges.

A) The Company should formulate the suitable controls in order to control the physical access to its information and communications technology environment, provided it include as a minimum the following:

1) Identify the users who are permitted to enter into the facilities of the information and communications technology environment, and specify the security conditions which should be observed upon entry into these facilities and document them within specific lists and review them continuously.

2) Grant the technical support employees from the external parties limited and temporary access rights for the information and communications technology environment facilities, and as needed only, provided that such access rights should be monitored and reviewed continuously.

B) The Company should place the suitable controls in order to access the networks, through specific access rights for every user separately, in a way fitting the importance and criticality of the applications and programs connected therewith or the increased risks of the sites occupied by the system users with due observance to the following:

1) Restrict access of users from outside the company through safe gateways and to specific programs.

2) Verifying and validating user's ID on the external networks.

3) The risks of operations and services provided through the networks.

Records

Article (12):

A) The Company should keep the historical data for all transactions made through its electronic systems according to the effective legal requirements, with the availability of the ability of retrieving them upon

request, provided that such data should contain what leads to the origin of the record, date and time of keeping such data.

B) The Company should keep all audit trails, operating and security events logs of the information and communication technology environment components for a minimum period of five years with due observance to the following:

1) Provide a mechanism to manage, analyse and monitor the records continuously.

2) Provide the required protection for the records to ensure its availability, integration and protection of records from change, loss, destruction, devastation and forgery by all users with all their authorities particularly system administrators.

Data Management

Article (13):
The company should produce and develop the necessary techniques for data management with due observance of the minimum limit of the following:

A) Utilize databases with suitable storage capacities and review such capacities to find out the extent of adequacy and increase the storage capacity whenever required.
B) Capability to store and retrieve data with speed, efficiency as well as ensure availability, integration and reliability of such data.
C) Setting the suitable protection controls for databases protection from unauthorized access.
D) Ascertain coding of all sensitive data upon movement and storage.
E) Define the mechanism of data storing, storage and processing sites and transferring as commensurate with the criticality of such data.
F) Formulate robust procedures to destroy the sensitive data including the utilized storage media, when the need for it does not exist anymore with due observance of the legal period for keeping such data.
G) Formulate the adequate procedures for tackling the errors of data management, and review the extent of sufficiency and efficiency of such procedures continuously.

Article (14):
The company should subject the data (whether the stored or transmitted) and backups of these data and particularly the sensitive ones to the proper encryption controls with due commitment to the following as a minimum:

A) Employ highly reliable coding controls to ensure the confidentiality of the sensitive data, whether being at the level of personal data or the data of the financial transactions pertaining to customers and those which are kept with a third party in the manner which ensures its none misuse.

B) Formulate and document the detailed policies and procedures, as well as review them periodically to organize the management of cryptographic keys including its creation, storage, utilization, stoppage, expiry, and renewal of its validity, archiving, reviewing and monitoring.

C) Employ sufficient and efficient security equipment such as the devices pertaining to the storage of cryptographic keys (HSM) and other tools, and systems that utilized for encrypting the company sensitive data in the stage of its transmission and guaranteeing the establishment and management of the secret keys used in the encryption in safely manner.

Backup and Restoration

Article (15):
The company should formulate procedures and mechanisms for backup to ensure the availability of the company's data provided that they must include the following as a minimum:

A) Backup copies of all databases, information, data and all configuration of the information and communications technology environment must be taken periodically and kept in special storage media and keeping the copies separate from their source.
B) Provide a suitable level of physical and logical protection of backup copies.
C) Testing the backup copies restoration in a manner consistence with the approved backup procedures by the company, and documenting the restoration procedures and results.
D) Examine the extent of sufficiency and effectiveness of the storage media, and it meets the company's requirements in supporting the restoration process.

Article (16):
The company should set the necessary procedures for ensuring not to make any unpermitted amendment on the source code copies, retain them in safe sites and under suitable protection levels.

High Availability

Article (17):
The company should ascertain the existence of sufficient controls to ensure the high availability of the information and communications technology environment, and particularly the critical systems with due observance of sufficient capacity, reliable performance, quick response time, scalability and ability to quickly recover the work.

Article (18):
The company should ensure the availability of the information and communications technology environment's components to reduce the single points of failure, which would lead to work breakdown and upkeep the equipment, software and backups networks required to quickly recover the work.

Article (19):
The company should endeavour to achieve the principle of multi communication channels between the various parties, where the various channels need to be provided by different communication service providers, to avoid the dealing risks with a single service provider.

Business Continuity

Article (20):
The company should establish a disaster recovery site, which geographically separated from the main site, to ensure the continuity of the company's work, in the event of occurrence of an interruption in the main site.

Article (21):
The company should put down a business continuity and disasters recovery plan, including mechanisms of building, testing, operating and updating this plan, as well as reviewing and assessing the results of the tests to ensure the availability of company operations at least annually and whenever needed thereto, taking into consideration the following:

A) Conditions of activating business continuity and disasters recovery plan, including the procedures of implementing this plan prior to its approval.

B) Procedures of business continuity and disasters recovery plan, which shows the matters to be followed and performed when there is a need to activate the plan.

C) Procedures describe the steps through which the information and communications technology environment is operated in the disaster recovery sites.

D) Recovery procedures which are to be followed to retrieve work to its normal position.

E) Timetable showing the place and time of examining the business continuity and disasters recovery plan and testing procedures.

F) Training and awareness activities that designed to ensure the correct understanding of business continuity and disasters recovery plan.

G) Duties and responsibilities of individuals towards implementation every part of business continuity and disasters recovery plan.

H) Determine the procedures of restarting the company operations and requirements of recovering the system, and determine the recovery time objective, recovery point objective contained in the business continuity and disasters recovery plan, formulate response scenarios in the event of failure of ability to resumption during this period.

I) Documenting the interruption periods of service, reasons of interruption, and the adopted procedures in tackling the reasons of interruption in special register.

Data Centers Management

Article (22):

The Company shall provide physical and environmental security controls for the data centers at the main and disaster recovery sites provided it include the minimum of the following:

A) Secure physical protection for the data centers from environmental risks, such as maintain certain levels of temperature degree, humidity and dust, prevention of water and fire risks, and endeavor to provide distributed cooling throughout the room in a manner suiting the distribution of equipment inside the room.

B) Secure the physical protection through safety doors.

C) Provide recorded television control for the datacenters entrance.

D) Maintain records for visitors and/or users of datacenters upon entry and exit.

E) The infrastructure shall be far and protected from the possible threats of floods, water leakage and sewage.

F) Provide electric generators, systems and UPS batteries with sufficient capacity to run the company's devices and operations (at least the sensitive), in the event the main power source was interrupted and use of multiple points to supply the main devices and its components with the electric power in order to avoid the risk of relying on a single source of energy and the switching between them will be automatic.

Change Management

Article (23):

The Company shall set out the necessary rules and procedures for the changes management that occur on the information and communications technology environment, and the rules of approvals thereon, execution, and review them so that these rules are implemented on the changes related to the systems, security, corrective actions, programs and operating systems updates.

Article (24):

Before implementing the changes on the production environment, the company shall conduct risk analysis and the impact of change on the information and the communications technology environment related to company business, and to determine whether such change will lead to security implications or problems in the compatibility of programs, systems and applications.

Article (25):

The Company shall ensure that the changes are approved by the authorized party of granting the authorities for conducting the changes, and shall examine and document the change testing plans.

Article (26):

The Company shall take backups of the systems or applications related to change, before starting the change process and formulate a plan to go back to a previous version of the system or application, in the event of occurrence of any problems during or after the change application or after that, and formulate recovery options to tackle the events that the change does not allow for the company to go back to the previous situation.

General Provisions

Article (27):

The Company and prior to granting the final license, shall execute vulnerability Assessment by a competent party and provide the Central Bank with a report showing the results of such examinations, the Central Bank has the right at any time to request from the Company to conduct any security test related to the system and infrastructure.

The Governor
Dr. Ziad Fareez